REMARKS

To date, the Examiner has not indicated that the subject matter of the information disclosure statement (IDS) filed 06/06/2006 has been properly considered. A copy of such IDS is submitted herewith. If the Examiner requires additional copies of any reference(s), applicant invites the Examiner to contact the undersigned. Documentation in the file wrapper of the instant application confirming the Examiner's consideration of the appropriate reference(s) is respectfully requested.

The Examiner has rejected Claims 1-4, 6-31, and 34 under 35 U.S.C. 102(e) as being anticipated by Makinson et al. (U.S. Patent No. 7,023,861). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to independent Claim 1, the Examiner has relied on items 14 and 16, and Figures 3, 5, and 8, as well as the figure below, from Makinson to make a prior art showing of applicant's claimed "processor positioned on a network adapter coupled between a computer and a network."

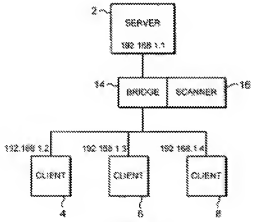

FIG. 4

Applicant respectfully asserts that the figures from Makinson relied on by the Examiner merely illustrate a network bridge and an associated network scanner. Makinson teaches that "[a] network bridge (14) has an associated malware scanner (16) that serves to concatenate portions of a data file from within data packets intercepted by the network bridge (14) and then scan the data file concerned before the data file is forwarded to its intended recipient by the network bridge (14)" (see Abstract – emphasis added). Further, Makinson discloses that "[t]he network bridge 14 includes respective network interface units 52, 54 at its two connection points to the network in which it is inserted" (Col. 5, lines 38-40 – emphasis added).

However, merely disclosing a network bridge used to intercept data packets, where the bridge includes two network interface units, as in Makinson, simply fails to even suggest a "processor positioned on a **network adapter** coupled between a computer and a network" (emphasis added), as claimed by applicant. Clearly, a bridge including two network interface units, as in Makinson, fails to suggest a "processor positioned on a **network adapter**" (emphasis added), in the manner as claimed by applicant.

Additionally, with respect to independent Claims 1, 14, 27 and 28, the Examiner has relied on Col. 5, line 67 – Col. 6, line 4 from Makinson to make a prior art showing of applicant's claimed technique "wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the computer and the network" (see this or similar, but not necessarily identical language in each of the foregoing independent claims).

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "[t]he processing performed by the central processing unit 58 may effectively carry out malware scanning by comparing a received data file against a collection of malware defining data, such as virus definition data" (Col. 5, line 67 – Col. 6, line 4 - emphasis added). However, merely disclosing malware scanning by comparing a file against a collection of virus definition data, as in Makinson, simply fails to suggest a technique "wherein the processor is adapted for virus scanning **and** content scanning of

network traffic transmitted between the computer and the network" (emphasis added), as claimed by applicant. Clearly, virus scanning with virus definition data, as in Makinson, fails to meet "virus scanning **and** content scanning" (emphasis added), in the manner as claimed by applicant.

Still yet, with respect to the independent claims, the Examiner has relied on the following excerpt from Makinson to make a prior art showing of applicant's claimed technique "wherein the virus signature files are stored on non-volatile solid state memory on the network adapter" (see this or similar, but not necessarily identical language in each of the independent claims).

> "The malware scanner 16 is illustrated in the form of a software based scanner using a general purpose computer formed of a central processing unit 58, a random access memory 60, a read only memory 62, a hard disk drive 64, a bridge interface unit 66, a user input/output unit 68 and a display driver 70 all connected via a common bus 72. This form of general purpose computer architecture is well known and operates with the central processing unit 58 executing program instructions that may be stored in one or more of the random access memory 60, the read only memory 62 or upon the hard disk drive 64." (Col. 5, lines 57-67 - emphasis added)

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches "a general purpose computer formed of a central processing unit 58, a random access memory 60, a read only memory 62, a hard disk drive 64..." (emphasis added). However, the excerpt from Makinson fails to rise to the level of specificity of applicant's claimed technique "wherein the virus signature files are stored on non-volatile solid state memory **on** the network adapter" (emphasis added), as claimed. Additionally, applicant notes that the memory taught by Makinson is found on "a general purpose computer," which does not meet any sort of "non-volatile solid state memory on the network adapter" (emphasis added), as claimed by applicant.

Furthermore, applicant notes that Makinson teaches that the "network interface units 52, 54 operate to receive all data packets on their associated network line and pass these packets to a packet analysis unit" (Col. 5, lines 41-43). However, network interface

units which pass data packets to a packet analysis unit for processing, as in Makinson, are not disclosed to include any sort of "virus signature files ... stored on non-volatile solid state memory **on** the network adapter" (emphasis added), as claimed by applicant.

With respect to independent Claims 14, 27, and 28, the Examiner has relied on the following excerpt from Makinson to make a prior art showing of applicant's claimed "receiving packets at a network adapter including a processor positioned thereon" (see this or similar, but not necessarily identical language in the aforementioned independent claims).

> "If step 24 indicateds that the data packet had a network layer protocol of a type suitable for scanning, then step 28 serves to identify the application layer protocol associated with that data packet. Again only certain types of application layer protocol (such as, for example, SMTP, FTP, HTTP, SMB or NFS) may be intended for scanning by the associated malware scanner 16 and these are selected for scanning by step 30. If the identified application layer protocol is not one that is to be scanned, then the data packet is again forwarded to its intended recipient via step 26. If the data packet has both a network layer protocol and an application layer protocol matching those that are to be scanned, then processing will proceed to step 32 at which the data packet is passed to the malware scanner 16 in order to be concatenated to form a data file to be scanned. Processing then returns to step 18 to await the next data packet." (Col. 4, lines 50-65 - emphasis added)

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "[i]f the identified application layer protocol is not one that is to be scanned, then the data packet is again forwarded to its intended recipient via step 26" and "[i]f the data packet has both a network layer protocol and an application layer protocol matching those that are to be scanned, then processing will proceed to step 32 at which the data packet is passed to the malware scanner 16 in order to be concatenated to form a data file to be scanned." In addition, Makinson teaches that "[a] network bridge (14) has an associated malware scanner (16) that serves to concatenate portions of a data file from within data packets intercepted by the network bridge (14) and then scan the data file concerned before the data file is forwarded to its intended recipient by the network bridge (14)" (Abstract – emphasis added).

However, disclosing that a network bridge intercepts data packets and that an associated scanner scans the data packets that have both a network layer protocol and an application layer protocol matching those that are to be scanned, as in Makinson, fails to suggest "receiving packets at a network adapter including a processor positioned thereon" (emphasis added), as claimed by applicant.

With respect to independent Claim 29, the Examiner has relied on items 14, 16, and 56 in Figure 8 from Makinson (reproduced below) to make a prior art showing of applicant's claimed "processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module."

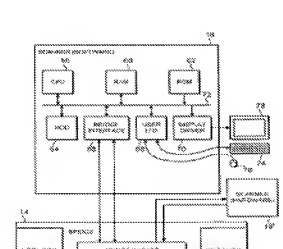

FIG. 8

Applicant respectfully asserts that the items and figure relied on by the Examiner simply illustrate the network bridge (14) which includes packet analysis unit 56, and associated malware scanner (16). However, Makinson's disclosure of a network bridge and associated malware scanner fails to suggest "a processor positioned on a network adapter coupled between a computer and a network" (emphasis added), as claimed by applicant.

Still yet, with respect to independent Claim 29, the Examiner has relied on the following excerpt from Makinson to make a prior art showing of applicant's claimed technique "wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the computer and the network."

> "If the test at step 40 indicated that a complete file has been received, then step 42 serves to apply the appropriate form of malware scanning using known malware scanning techniques, such as computer virus scanning (for viruses, Trojans, worms or banned files), e-mail scanning and the like. At step 44 a test is made as to whether or not the computer file has passed its scan. If the computer file has not passed its scan, then step 46 serves to repair or delete the file (as may be set by user configuration) and then issue an alert (such as sending an e-mail to a user configured address) at step 48. After step 48, or if the computer filed passed it scan as indicated at step 44, then step 50 serves to send the data file that has been scanned back to the network bridge 14 for it to be retransmitted to its intended recipient by the network bridge 14." (Col. 5, lines 22-36 - emphasis added)

Applicant respectfully asserts that the excerpt relied on by the Examiner merely teaches that "step 42 serves to apply the appropriate form of malware scanning using known malware scanning techniques, such as computer virus scanning (for viruses, Trojans, worms or banned files), e-mail scanning and the like" (emphasis added). However, merely disclosing that malware scanning includes computer virus scanning, and e-mail scanning, as in Makinson, fails to suggest that "the processor is adapted for discerning and virus scanning **and** content scanning of network traffic of interest transmitted between the computer and the network" (emphasis added), as claimed by applicant. Clearly, computer virus scanning, and e-mail scanning, as in Makinson, fails to meet "virus scanning **and** content scanning" (emphasis added), in the manner as claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be

shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the above reference, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows:

> "a processor positioned on a network adapter coupled between an end-point computer and a network, the network adapter capable of being installed on the end-point computer;" and
>
> "wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that by claiming that the "network adapter [is] capable of being installed on the end-point computer" (emphasis added), as claimed, applicant further distinguishes applicant's "network adapter" from Makinson's network bridge and malware scanner. As illustrated in Figure 8, Makinson's network bridge is clearly not a "network adapter capable of being installed on the end-point computer" (emphasis added), as claimed by applicant.

In addition, applicant's presently claimed "content scanning [that] includ[es] scanning for unwanted content other than viruses" (emphasis added), as claimed, also further distinguish applicant's content scanning from Makinson's disclosed "malware scanning using known malware scanning techniques, such as computer virus scanning

(for viruses, Trojans, worms or banned files), e-mail scanning and the like" (see Col. 5, lines 24-26 – emphasis added).

Again, the foregoing anticipation criterion has simply not been met by the above reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 35-41 below, which are added for full consideration:

"wherein the network adapter includes a Peripheral Component Interconnect (PCI) card" (see Claim 35);

"wherein the network adapter includes an Industry Standard Architecture (ISA) card" (see Claim 36);

"wherein the network adapter includes an Integrated Services Digital Network (ISDN) adapter" (see Claim 37);

"wherein the network adapter includes a cable modem adapter" (see Claim 38);

"wherein the network adapter includes a broadband adapter" (see Claim 39);

"wherein the unwanted content is selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation" (see Claim 40); and

"wherein the unwanted content includes harassing content, pornographic content, junk e-mails, and misinformation" (see Claim 41).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested. Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P056/01.187.01).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

Electronic Acknowledgement Receipt

EFS ID:	1068453
Application Number:	10029650
Confirmation Number:	2721
Title of Invention:	Embedded anti-virus scanner for a network adapter
First Named Inventor:	Anton C. Rothwell
Customer Number:	28875
Filer:	Kevin Joseph Zilka
Filer Authorized By:	
Attorney Docket Number:	NAI1P056/01.167.01
Receipt Date:	06-JUN-2006
Filing Date:	20-DEC-2001
Time Stamp:	18:27:52
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$160
RAM confirmation Number	399
Deposit Account	501351
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Descrip	File Name	File Size(B)	Multi Part	Pages
1	Information Disclosure Statement (IDS) Filed	NAI1P056_PRCIDS_related USapp_afterfinal_6-5-06_.pdf	189305	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	NPL Documents	NAI1P056_reference_P057AdvisoryAction_6-5-06_.pdf	465345	no	3
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	8162	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	662812		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of:	Group Art Unit: 2153
Rothwell et al.	Examiner: Chea, Philip J.
Application No.: 10/028,650	Atty. Docket No. : NAIIP056/ 01.187.01
Filed: 12/20/2001	
For: EMBEDDED ANTI-VIRUS SCANNER FOR A NETWORK ADAPTER	Date: June 6, 2006

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§1.56 AND 1.97(d)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The information disclosure statement transmitted herewith is being filed ***after*** a final action under § 1.113, or a notice of allowance under § 1.311, whichever occurs first, but before, or simultaneously with, the payment of the issue fee.

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

Applicants hereby state that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the statement after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in Section 1.56(c) more than three months prior to the filing of the information disclosure statement.

Applicants are including payment in the amount of $180.00 for the fee due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees or credit any overpayment to Deposit Account 50-1351 (Order No. NA11P056).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Reg. No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
Telephone: (408) 971-2573

Form 1449 (Modified)	Atty. Docket No. NAI1P056/01.187.01	Application No.: 10/028,650
Information Disclosure Statement By Applicant	Applicant: A. Rothwell et al.	
(Use Several Sheets if Necessary)	Filing Date: 12/20/2001	Group Art Unit: 2153

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A						
	B						
	C						
	D						
	E						
	F						
	G						
	H						
	I						
	J						
	K						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	L							
	M							
	N							
	O							
	P							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	R	Copy of Advisory Action from application no. 10/028,652 which was mailed on 03/23/2006
	S	
	T	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.